Telecommun Syst (2018) 67:553–575
https://doi.org/10.1007/s11235-017-0352-x

ESOT: a new privacy model for preserving location privacy in Internet of Things

Ikram Ullah[1] · Munam Ali Shah[1] · Abdul Wahid[1] · Amjad Mehmood[2] · Houbing Song[3]

Published online: 16 October 2017

Abstract The Internet of Things (IoT) means connecting everything with every other thing through the Internet. In IoT, millions of devices communicate to exchange data and information with each other. During communication, security and privacy issues arise which need to be addressed. To protect information about users' location, an efficient technique should be devised. Several techniques have already been proposed for preserving location privacy in IoT. However, the existing research lags in preserving location privacy in IoT and has highlighted several issues such as being specific or being restricted to a certain location. In this paper, we propose a new location privacy technique called the enhanced semantic obfuscation technique (ESOT) to preserve the location information of a user. Experimental results show that ESOT achieves improved location privacy and service utility when compared with a well-known existing approach, the semantic obfuscation technique.

✉ Amjad Mehmood
amjad.mehmood@kust.edu.pk

Ikram Ullah
ikram.comsats.cs@gmail.com

Munam Ali Shah
mshah@comsats.edu.pk

Abdul Wahid
abdulwahid@comsats.edu.pk

Houbing Song
h.song@ieee.org

1 Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan

2 Institute of Information Technology, Kohat Unversity of Science and Technology, Kohat, KP, Pakistan

3 Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114, USA

Keywords Location obfuscation · Location-based services · Location privacy · Internet of Things · Service utility

1 Introduction

IoT is a pervasive concept in which various things in the environment using wireless and wired connections interact and cooperate with other things and objects to share services and achieve common goals. The concern of IoT is making the world smart enough such that real objects create a smart environment in which transport, energy, healthcare system, smart grids and other area/fields of life become more intelligent. The main aim of IoT is to connect things with any other things, at anytime and anywhere to share resources and information [1–3].

The global network infrastructure of IoT enables the data communication capabilities such as autonomous data capture, event transfer, network connectivity and interoperability by connecting physical and virtual objects. The increased accessibility and connectivity of IoT devices in the communication network has become susceptible to security threats, i.e. spoofing, tempering, repudiation, confidentiality and privacy of users [4]. The privacy of users can be location privacy and query privacy. The query privacy relates to the mining of sensitive information. The location privacy is the protection of location information of user's sensitive information such as residence location, behaviour, health status and other sensitive information [5].

IoT devices have a built-in GPS system for positioning of location information. The user may issue a query to location based services (LBS) for location information. The query may be for a location of interest—for example, the nearest restaurant, hospital, park or other places. The query contains the identity and location of the user. The convenience of using LBS services creates issues of privacy risk. Based on the provided information, an adversary could easily link the identity and location of the user to get more private information [6]. Security and privacy are a critical measure to consider for information gathering and broadcasting. This information and data must be secure from illegal and unauthorized access [7].

The IoT devices which we use in offices, homes, streets and buildings are connected with each other and to the Internet, constantly sending information. The data exchanged contain sensitive information about a person. This information may be leaked and produce serious privacy issues. However, location information of devices is important to protect the privacy of devices users [8].

A location privacy protection proposal can be divided into three broad methods. The first method is based on anonymization of location based on temporal and spatial clocking to protect the real location of the user. The second concept in research work is location obfuscation, an approach based on slightly blurring or adding noise to the actual location of the user to guard against privacy attacks. The third method is centred on private information retrieval (PIR) [9]; presently PIR is not easy to apply in a real scenario.

Revealing the actual location of a person could create several threats, like harm to social status, damage of property, victims of physical violence and blackmail [10]. In such a case, location privacy becomes a critical issue to tackle in IoT. In this research, we aim to preserve location privacy in the IoT scenario while communicating with LBS. This research work is the extension of our published paper [11]. The main focus of our research work is using obfuscation to enhance the existing semantic obfuscation technique (SOT) approach [8].

In this paper, we aim to propose an obfuscation approach named as ESOT which protects the location privacy in the context of IoT. We introduce sensitivity levels and user privacy requirements to enhance location privacy protection level. Our proposed approach achieves balance between privacy protection and service utility. The rest of paper is organized as follows. Section 2 presents the literature review of existing location privacy techniques and approaches. The security of obfuscation function is analyzed in Sect. 3. Section 4 presents motivation and contribution. Section 5 contains details of our proposed method, the enhanced semantic obfuscation technique (ESOT). Section 6 consists of the tested results of ESOT. Section 7 contains performance results comparing ESOT with SOT [8]. The results are analysed in Sect. 8 and the paper is concluded in Sect. 9.

2 Related work

In this section we describe the detail of location privacy techniques, which is comprised of anonymization techniques, obfuscation-based techniques and noise-based techniques.

2.1 Techniques based on anonymization

K-anonymity is one of the basic techniques for protection of privacy proposed for the first time by Sweeney [12]. The k-anonymity model addresses the re-identification problem during broadcasting sensitive information for the research objective. Gedik and Liu [13] presented a new architecture for the protection of location privacy from several threats due to unrestrained practice of LBS. This strategy contains a personalized k-anonymity prototype and a suite of algorithms based on anxiety to protect privacy. The distinctive feature of this design is the elastic personalization privacy to sustain k-anonymity for wide-ranging mobile clients. The prototype is designed to be on a trusted platform of an anonymization server.

Yao et al. [14] presented a location protection method for ubiquitous computing surroundings called ClusterCloak. This approach is based on personalized k-anonymity to guard the locality privacy of mobile users. A mobile user can get the desired level of anonymity with the help of clustering. The precise position of the user is swapped by means of minimum bounding rectangle (MBR). Analysis shows that ClusterCloak accomplishes high resilience against location privacy attacks. Palanisamy et al. [15] presented a new approach, MobiMix, a road network based on a mix-zone approach to protect the location of mobile users throughout travelling. Numerous aspects such as zone geometry, statistical behaviour of the population, spatial constraint, and temporal and spatial resolution are considered to build mix-zones. This structure provides efficient results for anonymization and resistance to threats compared with related methods.

Wang et al. [16] presented mobile user location privacy in active and varied scenarios, reinforcing it to articulate the location awareness and location privacy protection (L2P2) problem. The problem is additionally distributed into basic and enhanced problems, and a distinct algorithm offered for each problem. The main concern of L2P2 is to define the cloak area for each user request. In this way, varied user privacy requirements are satisfied across temporal and spatial dimensions. Pan et al. [17] proposed an incremental group-based hiding procedure, ICliqueCloak, by approving privacy metrics such as k-anonymity and cloaking granularity to protect against location-based attacks in mobile facilities. The problem is formalized with a graph model and transformed to reveal the k-node clique's problem in a graph. ICliqueCloak is an incremental group-based approach which generates a cloaked region. Experimental results show that the algorithm provides efficient location privacy protection.

Vu et al. [18] introduced a novel technique grounded on locality sensitive hashing (LSH) which divides the user location into clutches called spatial cloaks. The proposed method is comprised of algorithms to create spatial cloaks and a k-nearest neighbour (KNN) search of points of interest (POI) to protect location information. Che et al. [19] exploited the privacy matter in LBS and proposed a double active spatial cloaking algorithm for protecting mobile user location privacy in the peer environment. The algorithm accomplishes the desired anonymity objective in less time by two methods: peer location information and storing location records for a period of time.

Yang et al. [20] introduced a decentralized context sensitive personalized collaborative (CSPC) cloaking scheme for location privacy protection. The exact location of the service requester is hidden through collaboration by the cloaking region. The user can manage and set privacy requirements based on various contexts for k-anonymity requirements. A privacy profile is maintained to record privacy requirements. K-anonymity, l-diversity and cloaking granularity are satisfied in this approach. Location cloaking algorithms do not reflect the outcomes of constant location updates during processing. Wang et al. [21] introduce an anonymity algorithm to guard against velocity-based attacks. It is based on a greedy approach to protect the location privacy of the user.

Niu et al. [22] present a caching-based scheme for the protection of location privacy. Their work specifies the requirements of caching to improve privacy. An entropy-based metric is used to check the caching effect on privacy. Two caching-aware dummy algorithms, the caching-aware dummy selection algorithm (CaDSA) and the enhanced CaDSA, are designed to enhance location privacy. The concept of k-anonymity is used in dummy selection algorithms, which protect the privacy of the contributor who submits queries to LBS.

Chen and Wei [23] proposed a distance based location privacy scheme SafeAnon in Vehicle ad-hoc Networks (VANETs). This technique uses anonymization to protect location privacy of vehicle and does not need trusted authority. A proactive based V-routing protocol is proposed for ad-hoc networks to protect the location privacy of communicating parties in [24]. Their routing protocol supports user anonymity and communication anonymity of entities in a multi-hop communication network and preserves the location privacy in the network.

2.2 Randomized noise-based techniques

In this section we discuss those techniques which are based on random noise added to the original location. This random noise changes or blurs the original location in such way that the adversary cannot acquire the actual location of the user.

Wightman et al. [25] introduce N-Rand, N-Mix and N-Dispersion techniques for the preservation of location privacy. N-Rand and N-Dispersion attain better average distance from the original location compared with classic techniques. The foremost discovery of the authors is that the addition of suitable noise may offer effective resistance against attacks. For this purpose, Dini and Perazzo [26] presented an obfuscation operator UNILO for location privacy protection, which adds a special random noise for the highest uniformity. The property of uniformity is verified by presenting an adversary model.

Wightman et al. [27] introduce the θ-RAND random point generation approach. It is greatly resilient to noise filtering attacks. It is planned for proactive applications which continually update the locality to LBS. In this obfuscation technique, random circle sectors with radius rmax and angle θ are used to generate random points.

Wightman et al. [28] presented a Pinwheel random noise-based location obfuscation approach for the protection of location information. This approach is planned for the continuous tracking and updating of applications. It is a pinwheel-like shape algorithm generating randomized points. Pinwheel reduces the chances of an exponential moving average (EMA) based filtering attack by generated noise. Zurbaran et al. [29] present a new random noise-based technique Near-Rand for location protection. A random point is produced in a square area and computes the average point adjacent to the original location of user. Near-Rand is not limited to a circular area, but searches points in the distributed cloud randomly.

Xi et al. [30] introduced a two-way random walk algorithm Greedy Random Walk (GROW). It reduces the chances for an adversary to obtain location information in wireless sensor networks. A backtracking model is used for the verification of privacy protection. With the help of a Bloom filter and local broadcasting, basic random walk is improved. Quercia et al. [31] proposed a mobile application SpotME that estimates the number of people preserving privacy in a geographical location. User report a very large number of inaccurate locations in addition to the real location. The randomized response algorithm selects an erroneous location. SpotME has negligible computational and storage overheads.

Kachore et al. [32] introduced three kinds of obfuscation function used to obfuscate users' path and location of LBS. These functions are ellipsoidal random obfuscation function (EROF), modified random obfuscation function (MROF) and grid obfuscation function (GOF). EROF is a non-reversible obfuscation function in which it is impossible to reacquire the original location and path of the user from the obfuscated path. MROF and GOF are reversible functions in which the original path can be accessed from the hidden path.

A location privacy preserving mechanism (LPPM) must contemplate three fundamental features: user privacy requirements, knowledge and abilities of adversary, and tolerated service quality. Shokri et al. [33] introduced an optimum LPPM for LBS which gives users a service quality constraint against an adversary optimal inference algorithm. The authors formalize mutual optimization with location privacy versus correctness of localization by using Stackelberg Bayesian games. It reports that an adversary could not observe that the location has been disturbed by the user.

2.3 Other location preservation techniques

In this section, we discuss the techniques which are based neither on k-anonymity nor obfuscation. The details are given below.

Wang et al. [34] combine k-anonymity and obfuscation-based techniques to proposed a new scheme, distributed user-demand-driven (DUDD), for location privacy. The sub-cloaking area is selected within a cloaking area produced by an anonymization server. In this architecture, location privacy is employed on the server side. Quality of service is dedicated to LBS. Miura and Sato [35] introduced a node density-based location privacy technique to protect privacy of location. The scheme is a hybrid combination of a dummy node and a cloaking region. Considering the density of node cloaking, the degree of location is changed vigorously. The greater the number of dummy nodes, the lower will be the quality of service.

Zhu et al. [36] proposed a dynamic pseudo-ID system in which a link between user identity and location is broken through unlinkable pseudo-IDs. The verification and authentication of dynamic pseudo-IDs is through certificates. The adversary will experience great difficulty getting information about the user's route.

Zhou et al. [37] proposed a multi-routing random walk strategy to protect sensor's location privacy in the context of IoT. For privacy protection, the random walk is improved by using multi routes and a Bloom filter. Khoshgozaran et al. [38] presented an approach based on private information retrieval (PIR) for processing a range and k-nearest queries, to provide stronger location privacy protection as compared to other cloaking and anonymity approaches. Agir et al. [39] proposed a user-side privacy protection scheme which adaptively set the parameters for protection of personalized privacy requirements in a measurable manner. The scheme provides both location privacy and data utility. Oh et al. [40] proposed a new mechanism, Phantom, to prevent an adversary from location tracking by generating fake locations. Phantom allows users to generate confusion about their location by generating ghost transmissions from various locations.

2.4 Obfuscation-based techniques

In this section, we provide details of location privacy techniques based on obfuscation. Obfuscation is a privacy-preserving technique in which the original location is blurred or slightly changed to another location. Various techniques have been proposed in this category. An overview of such techniques is given below.

Context information is very sensitive and needs to be protected efficiently. Wishart et al. [41] proposed an obfuscation technique based on using an ontological description and the provision of numerous obfuscation levels for random classes of context information. This technique adjusts context information to meet user disclosure requirements. It provides various levels of obfuscation to protect user location information. Ardagna et al. [42] presented a privacy enhanced approach based on spatial obfuscation to protect the location privacy of users. The authors also proposed a proper and essential way to define privacy preferences and an accuracy metric for location. The metric defines various degrees of privacy protection.

Ardagna et al. [43] present several obfuscation operators for location privacy protection, also considering the accuracy of location measurement and user privacy requirements. The obfuscation operator can be used individually or in combination to provide security of location privacy of the user. The results prove that these operators provide more efficient privacy protection than current solutions. Various existing techniques are based on geometric knowledge of location, which does not provide efficient privacy protection against attacks in a spatial context. In this scenario, Damiani et al. [44] presented a semantic aware obfuscation method for the preservation of location privacy. The new framework contains an algorithm for location obfuscation and the safeguarding of sensitive location in a privacy model.

Seidl et al. [45] introduced an obfuscation technique, voronoi masking, to protect the privacy of household level data. The authors associate the performance of this method with other three techniques, which is better than other obfuscation approaches for protecting point distribution. The authors also examine four other spatial obfuscation techniques for surveyed household data. Cross-k function and cluster analysis are used to measure household privacy. Ilyas and Vijayakumar [46] presented a location privacy model (LPM), a distributed location obfuscation method for location privacy protection in LBS.

Zhang et al. [47] introduce a path-based access control technique to obfuscate location information. The notion of access probability is used to ensure accurate obfuscation parameters. This obfuscation model efficiently protects information location privacy in the mobile environment. Skvortsov et al. [48] present a map-aware position-sharing scheme to manage users' obfuscated positions on location services. The basic idea is to split the precise user position into a set of imprecise position shares. These shares are divided among the location services of various providers. In this way, the location privacy of the user is preserved, as each location service stores only one share. If location services are compromised, this will not reveal the precise location of user. Wightman et al. [49] introduced a new obfuscation scheme, Matlock, which is lightweight and reversible. This scheme is based on matrix obfuscation. Matlock has low computation overheads and obfuscates the location in both the temporal and spatial dimensions.

Xiao et al. [10] proposed LocMask, a scheme for location privacy protection in an android system. It has privacy levels based on sensitivity of location. This scheme manages the location profile of the user and records the user's mobility pattern. The location is ranked based on the visiting frequency of the user. Users' top locations (home, office) need more protection and should be included at a very high level of sensitivity.

Location obfuscation is one technique for preserving location privacy by degrading service quality. Le et al. [50] propose Semantic Bob-tree for location privacy protection at the database level. The tree nodes contain semantic-aware information. The privacy profile is maintained to define the sensitivity level. The range of sensitivity level is [0, 1], where the value 0 considers that the location is not sensitive and the value 1 is the highest user sensitivity region for location services. The user has the option to select the level of sensitivity based on his/her location. Damiani et al. [51] introduced a new privacy model and architecture framework, PROBE, for semantic location privacy in personalized cloaked regions. Privacy profiles of user-cloaked locations are maintained. The sensitivity of a region is defined with respect to the semantic location user. The user must specify the location sensitivity and privacy preference in their privacy profile.

Haadi [52] introduced a novel location privacy scheme focused on vagueness of human perception of nearness. The notion of degree of vagueness used in this work makes it strong against privacy attacks. Human perception in this scheme allows entities directly to define their privacy preferences using vagueness/nearness for each region. Apps et al. [53] propose a framework of location privacy for an android system in which various obfuscation algorithms can be integrated. Users of LBS can add various inaccuracies to their location through the app based on location use cases. Location obfuscation has categories in levels—e.g. city level obfuscation, street level obfuscation. This scheme maintains a balance between location privacy and the service required by user.

Table 1 shows various location privacy techniques and their features.

3 Security analysis of obfuscation function

Obfuscation is a type of method used to degrade the quality of the information deliberately in such a way to hide and secure the privacy of user in the IoT. The obfuscation function could be used to preserve the location privacy of person while communicating with LBS for finding location of its interest. The obfuscation is the imperfection of deliberate degradation of spatial information quality. The imperfection recorded in literature may be imprecision, inaccuracy and vagueness. Imprecision is the lack of specificity in information, inaccuracy is the lack of correspondence between information and reality, while vagueness in information relates to boundary cases [55]. These three types of imperfection can be used for obfuscation function to preserve the location privacy.

The main security strength of obfuscation is the property of reversibility which makes it difficult for an adversary to reverse engineer the obfuscated data set. Obfuscation can also provide multilevel data protection based on the various demands of the end users. The paper [56] describes three main features of obfuscation, i.e. reversibility, specification and shift. Reversibility property of the obfuscation describes the complexity to reverser engineer the obfuscated function which shows its robustness in terms of data hiding. Specificity defines parameters for obfuscation mechanism, while the shift defines process of obfuscation. Specificity may be absolute or relative. In shift parameter, the data could be obfuscated with help of either constant or random fashion. The main purpose of using these features is to increase robustness of obfuscation mechanism and to make it difficult to be reverse engineered.

Obfuscation function has potential to extend the location privacy competencies. The anonymization based mechanisms have the problem of authentication and personalization. While obfuscation mechanism improves the protection level of location privacy. Also, it avoids problems faced during the authentication and personalization in anonymization mechanisms. An obfuscation mechanism does not depend on central controller to administer privacy policies, which make it suitable for distributed environments [57].

Form security analysis point of view, it is stated that obfuscation mechanism is efficient to provide higher level of location privacy protection. The strength of anonymization depends upon the numbers of users in a group. Higher the number of elements or users in a group, higher will be the level of privacy protection. However, it is difficult task to group higher number of users in a concerned area. For this purpose, we use obfuscation function to preserve the location privacy. Another benefit of obfuscation is the difficulty to reverse engineer it. We used obfuscation function in such a way that it keeps balance between privacy protection and quality of service during communication with LBS. Our obfuscation function combines both imprecision and randomization features of obfuscation.

Table 1 Overview of some existing location privacy techniques

References	Anonymization	Obfuscation	Technique	Features	Limitations/deficiencies	Application
[14]	✓		ClusterCloak	Accuracy, robustness, lower complexity, improved quality of service	Does not address MAC layer	Pervasive computing
[54]		✓	DLDA agent	Context-aware adoptive, obfuscation of location	Restricted to specific location	General IoT devices
[19]	✓	✓	Self-clock area (SCA)	Greedy approach, fewer computation overheads, decentralizing location	Assumes trusted third party entity	Mobile client
[8]		✓	Semantic-based	Geographical knowledge, ontology based, lower prediction rate	Restricted to specific location	IoT devices
[43]		✓	Obfuscation operator	Better protection, robustness	Only deals with geometry of location; does not consider geographical features	Mobile client
[41]		✓	Context-aware	Variable levels of obfuscation, supports ontology	Reveals activities of user to buddies during context collection	Pervasive computing
[18]	✓		LHS-based cloak	Moderate computation complexity, superior performance	Overhead to keep data anonymous	Mobile devices
[42]		✓	Spatial obfuscation	Accuracy of location measurement, expression of users' privacy preferences	Attacker makes use of match map to get precise known position	Mobile client
[16]	✓		L2P2	Polynomial-time heuristics dynamic and diverse privacy requirements	Fails to protect trace privacy	Mobile client
[15]	✓		MobiMix	High-level resilience to attack mix-zone construction	Does not consider background knowledge attack	Mobile client
[17]	✓		ICliqueCloak	Generation of cloaked regions, incremental cloaking, formalizes problem on graph model	Small price is paid to defend attack	Mobile services
[13]	✓		CliqueCloak	Perturbation engine, high resilience to location privacy threats	Anonymity server has knowledge of user position	Mobile client
[26]		✓	UNILO	Uniform obfuscation, addition of special random noise	Lack of experiment with real human mobility traces	General
[27]		✓	θ –RAND	Noise-based technique, circular sector with radius and angle θ, greater variability	Restricted to circular area, which limits variability	Cell phone
[28]		✓	Pinwheel	Noise-based, higher level of asymmetry in noise generation, larger variability, reduced effect of EMA filtering attack	Restricted to circular area, which limits variability	Mobile client/general

Table 1 continued

References	Anonymization	Obfuscation	Technique	Features	Limitations/deficiencies	Application
[29]		✓	Near-Rand	Noise-based, calculates average nearest point in square area	May limit variability	Cell phone
[31]		✓	SpotME	Robust against injection of false location, negligible computational and storage overheads	Communication overheads	Mobile phone
[49]		✓	Matlock	Light-weight, provides high security, also reversible	Low complexity limits it to run on constrained devices	Mobile phone
[10]		✓	LocMask	Privacy profile management, location sensitivity levels, balance between privacy and utility	Cannot be applied to advanced privacy protection techniques	Android system
[50]		✓	Semantic Bob-tree	Privacy profile is maintained, sensitivity range in [0,1], index tree structure	Reduced quality of services, increased storage cost	General
[20]	✓		CSPC	Personalized privacy requirements, supports k-anonymity and l-diversity	Computational overheads (time consuming)	Mobile client
[34]	✓	✓	DUDD	Balance between privacy and quality of service, combining obfuscation and anonymization, privacy protection on server side	Need for integrated metrics for evaluation of user demands	Mobile communication network
[21]	✓		Greedy anonymity algorithm	Greedy approach, defends against velocity-based attack, can apply directly to continuous query-based systems	Increased query processing and communication cost for large value of k, l	Mobile client
[22]	✓		Caching-based scheme	Entropy-based privacy metric is used, dummy location selection algorithm	Assumes user has constant and isolated privacy requirements	Mobile client
[52]		✓	Vagueness-based	Based on human perception, vagueness degree, applicable to various architectures	Too much noise decreases service quality	General architecture
[44]		✓	Semantic-aware obfuscation	Sensitive location privacy model, efficient safeguard against privacy attacks	Bottleneck of this technique is required dedicated trusted server	Mobile client

4 Motivation and contribution

Location privacy is an important problem in respect of IoT. The connected devices in IoT exchange information with each other. During communication between these devices, the threat may arise to obtain location information about the user. To preserve the location privacy of the user, several obfuscation techniques have been proposed. SOT [8] is one technique that addresses the location privacy issue in respect of IoT. Certain limitations are found in SOT, including SOT location obfuscation being restricted to a specific location and it being difficult to apply all over the world. There is variation of location in different countries of the world. The second limitation is that SOT measures only the prediction rate that the location is fake or obfuscated. Our contributions in this paper are as follows.

1. We enhance SOT [8] to be applicable globally.
2. We introduce privacy sensitivity levels based on user choice.
3. We reduce levels of obfuscation to improve location privacy and location service utility.
4. We introduce reasonable ranges of obfuscation to achieve a balance between privacy and service utility.

5 Proposed enhanced semantic obfuscation technique (ESOT)

The proposed ESOT technique is designed to preserve the location privacy of general IoT devices. The technique is based on the semantics of user or device location in IoT. The main objective of the proposed approach is to hide the original location of devices from an adversary who is interested in the user's location to reveal private information. Our intention is also the protection of the user's location information from LBS, as in our scenario LBS cannot be taken as a trusted party. Obfuscation is a technique which is used for protection of the location privacy of the user. Obfuscation blurs the real location of the user to some other location near to the original location. The existing research clearly lags in the protection of location privacy and a balance between privacy and service utility.

SOT [8] obfuscation consists of five levels, while in the proposed technique it is reduced to three levels for utility purposes. In SOT [8], level 4 and level 5 have location obfuscation at state and country level respectively—for example, the user's original location is Australia and the obfuscated location will be another country such as New Zealand, which badly affects the location services required by the user. The architecture of ESOT is shown with the help of Fig. 1. ESOT consists of privacy preferences, which must be given by the user while querying LBS. Based on user privacy preferences, the concerned obfuscation level is selected to obfuscate the current location of the user. Each level has its own obfuscation area to hide the original location of the user. Each area has several points to hide the location. ESOT selects one point among these points to obfuscate user location. This section consists of privacy profile generation, obfuscation levels, the system model, an ESOT flowchart and algorithms of the proposed technique.

5.1 Privacy profile generation and sensitivity levels

User privacy preferences are stored in a privacy profile with the passage of time based on the sensitivity of locations. A privacy profile generator is used to create and manage sensitivity of location. The user has the option to give preference to his location. Privacy preferences of user location are divided into three categories: low sensitivity, medium sensitivity and the most sensitive location, as in the papers [10,50]. The user must explicitly give his/her privacy preferences/requirements to get the required privacy protection level. High sensitivity locations require high protection for location privacy. Low and medium categories require low and medium location privacy protection respectively.

Those locations of users which are less visited by the user are considered to be in the low sensitivity category. The user ascribes importance to a location based on his own choice, dependent on user visits to a certain location. A low sensitivity location involves casual visits of users while using location services, including places like shopping malls, parks, cinemas, etc. A low sensitivity location is obfuscated in the first level—i.e. obfuscation level 1—which has low proximity.

A frequently visited location is considered a medium sensitivity category. A medium sensitivity location includes visits to playgrounds, religious places, etc. The sensitivity level is higher than a low sensitivity location due to which it is obfuscated in wider proximity as compared with the first level. It depends on user choice to categorize his location based on his own importance.

High sensitivity locations have much importance compared with the other two categories. The user does not want to reveal such a location. The adversary can easily obtain a lot of personal information from these locations. Revealing such information may generate higher damage to the user, due to which it needs higher protection. Wider proximity is required to protect the privacy of these locations. High sensitivity locations may include home, hospital, office location, etc. Privacy sensitivity levels are also defined with the help of Algorithm 4.

5.2 Levels of obfuscation

ESOT has three obfuscation levels—level 1, level 2 and level 3. The reason for reducing levels of obfuscation to three

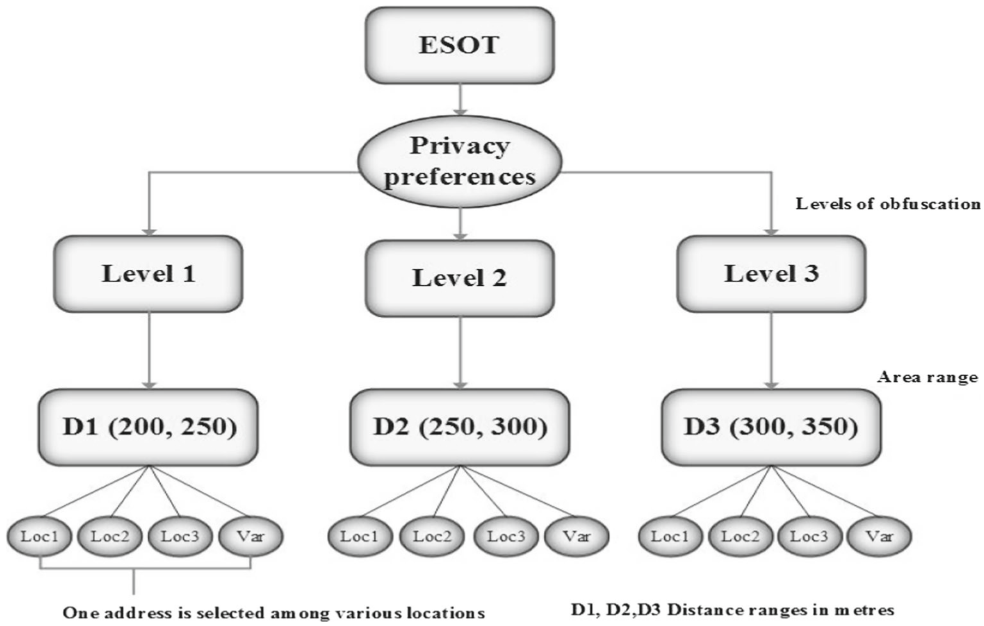

Fig. 1 ESOT basic architecture

is for service utilization. Let's take an example: a user is interested in finding the location of the nearest hospital or restaurant to his/her original location. For this purpose, the user makes a request to LBS. His/her request query is first passed through the obfuscated technique (ESOT) in order to be received by LBS. Based on the received location, LBS calculates the required location. If the user's original location is converted to an obfuscated location which is outside his/her state or country, then how would he get the required service? That is the main reason we reduced obfuscation to three levels. The levels of obfuscation have certain distance ranges to hide the original location of the user.

In level 1, the original location is converted to an obfuscated location in range D1, a 200 to 250 m circular area. The first level hides a less sensitive location, due to which it searches addresses in a small area. The original location is compared with other locations lying in range D1. If they are the same, then the search is extended beyond D1. One important point is that if the area is rural (rural areas are not efficiently plotted on Google Maps) and does not contain different addresses in this small area, then ESOT gives the nearest location which is different from the original location.

Level 2's obfuscated range, D2, is an area of between 250 and 300 m. A medium sensitivity location is obfuscated at this level. It has a wider proximity and area range compared with level 1. If a location is not found in its range, then the search is extended beyond the level 2 range to find a location for obfuscation. Level 3 has an obfuscation range, D3, of between 300 and 350 m. The high sensitivity category of location comes under this level. Levels of obfuscation are also defined with the help of Algorithm 3.

5.3 System model

Our proposed system model consists of three entities: IoT devices, obfuscation engine and LBS, as shown in Fig. 2. In this model, the user of the IoT device asks LBS for a location. This request must be passed through the obfuscated engine ESOT. The obfuscated engine comprises privacy preferences and obfuscation levels. This engine obfuscates the user's original location according to sensitivity levels. The obfuscated location is communicated to LBS for the location of interest to the user of IoT. After that, the location request query is forwarded to LBS for necessary correspondence. LBS calculates the location of interest to the user and sends it back to user. The original location is hidden by another location which protects the location information of the user from an attacker or adversary. In the system model, LBS is assumed not to be a trusted party and the location must be hidden from LBS. The user initiates a query to LBS for location services. The original location of the user is obfuscated through ESOT. The service provider receives the location of the user, but this location is not the original location of user: it is an obfuscated location. LBS provides a service to the user based on the user's current location. The user initiates a query Q (L, S) to LBS; this query is obfuscated with ESOT and query Q (L′, S) is sent to LBS. LBS calculates services for the user and replies to query Q (Ls, S) to the user, where

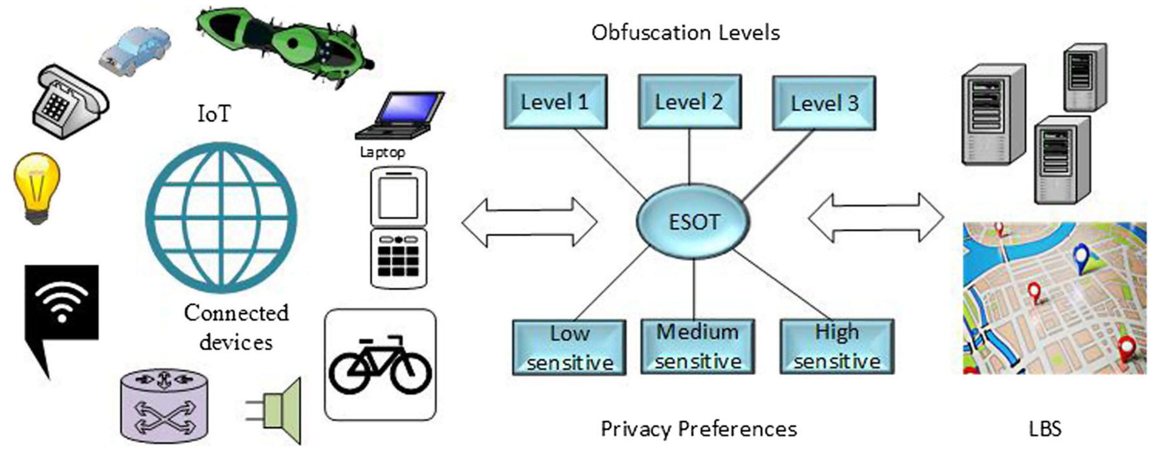

Fig. 2 Details of ESOT system model

L is the original location, L' is the obfuscated location and Ls is the service requested by the user.

5.4 Flowchart of ESOT

The flow diagram of our proposed ESOT scheme is shown in Fig. 3. The system starts with privacy preferences. Privacy preferences must be given by the user in order to work further on levels of obfuscation. The three levels of obfuscation have to be chosen according to user location preferences. Each level has its own start-up area range to search for an alternative location instead of the original location for privacy preservation purposes. The search extends beyond the boundary area in each level if a location is not found in its own region. When the search is successful, the original location is converted to an obfuscated location at the end of the flowchart.

5.5 Algorithms of ESOT technique

The main procedure of ESOT is given by Algorithm 1. The algorithm takes the original location L as input and produces the obfuscated location L$'$, which is different from the original location. The user must specify privacy preferences based on level of sensitivity to obfuscate the location in the relevant range. The obfuscation function is executed to convert the original location to another location.

The obfuscation function is explained with the help of Algorithm 2. This function searches locations in a certain range. The original location and the obfuscated location are compared to check similarity. If a location is not found, the search is extended beyond each range level until a location is found. The levels of obfuscation are selected based on user location sensitivity. Every level has a certain range to convert the original location into a hidden location. The procedure for obfuscation levels is described with the help of Algorithm 3.

The main procedure of location sensitivity levels is shown in Algorithm 4. This algorithm contains three levels of location sensitivity: high sensitivity location, medium sensitivity location and low sensitivity location. The level of sensitivity depends on the user's choice—which location is more sensitive to the user compared with other locations. Higher sensitivity locations must be obfuscated in a wider proximity.

Algorithm 1: Main Procedure of ESOT

```
L⟵Original Location
L'⟵Obfuscated Location
Pf (0,1,2)⟵ Privacy Preferences
R1, R2, R3⟵Ranges of concerned levels
Obfuscate ()⟵ Function to obfuscate location
   for pf⟵ 0 to 2 do
      if pf⟵ 0 then
          Find location in Range R1
          L'⟵ Execute obfuscate(L)
         else
        if pf⟵ 1 then
              Find Location in Range R2
              L'⟵ Execute obfuscate(L)
         else
          if pf⟵2 then
              Find location in Range R3
              L'⟵ Execute obfuscate(L)
           end if
         end if
      end if
    end for
    Return L'
```

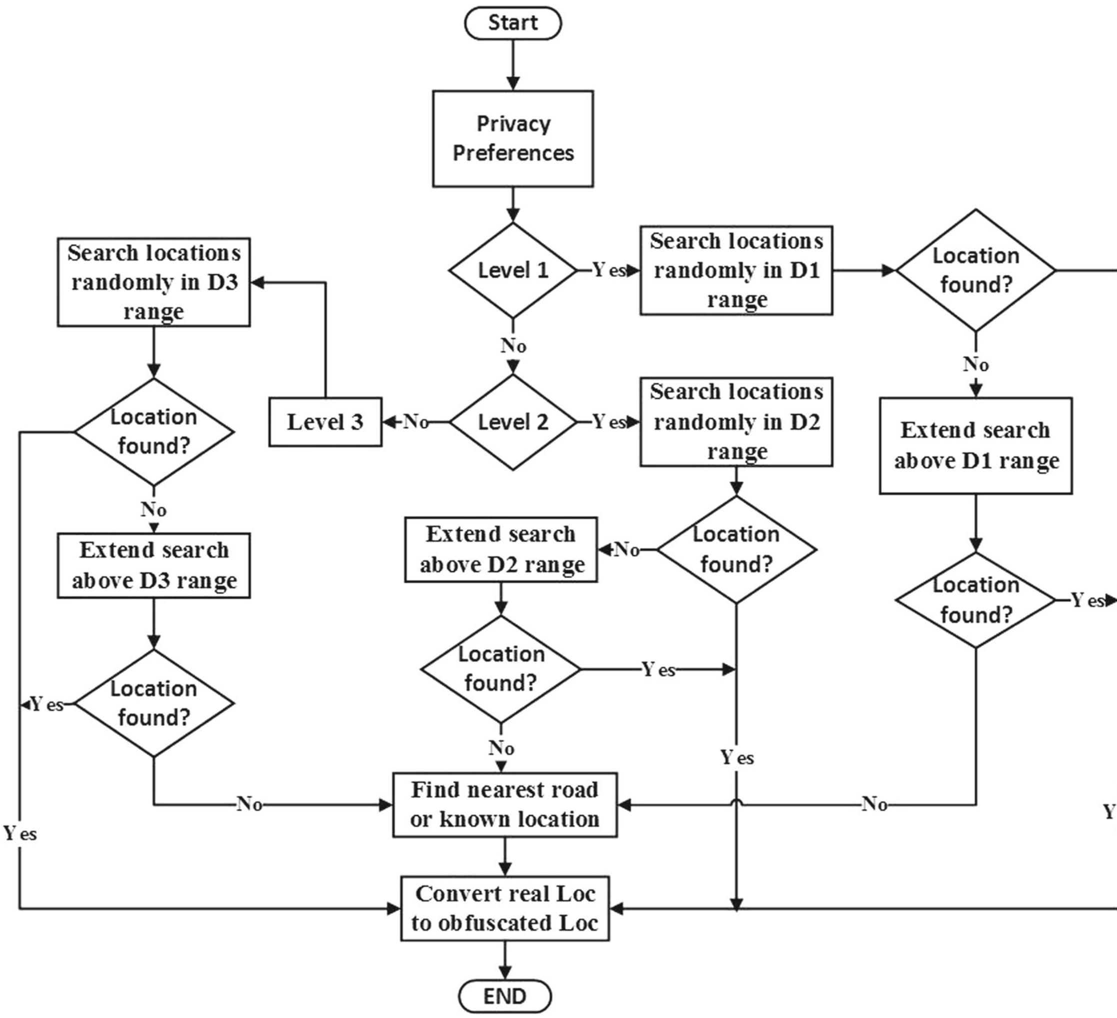

Fig. 3 Flowchart of ESOT

Algorithm 2: Obfuscation function

```
L⟵Original Location
L'⟵ Obfuscated Location
Find Location in certain range
  if Location == True then
   Compare with Original Location (L)
      if L == L' then
        Extends search above certain range
        Continue search until location is found
      end if
      Convert Original Location (L) to Obfuscated Location
      (L')
  end if
```

Algorithm 3: Obfuscation Levels

```
Location ⟵ location to be searched in certain range
Level ⟵ Levels of obfuscation
R ⟵ Area of range for location hiding
   for I ⟵ 0 to 2 do
     if level == 1 then
          Find Location in Range R1
      else
       if level == 2 then
         Find Location in Range R2
         else
         if level == 3 then
              Find Location in Range R3
          end if
       end if
      end if
     end for
     Return Location
```

Algorithm 4: Privacy Preferences of Sensitivity Levels

```
HS ⟵ High Sensitive
MS ⟵ Medium Sensitive
LS ⟵ Low Sensitive
Sensitivity Levels (HS, MS, LS)
LOC ⟵ Location of user
   if LOC == HS then
       Place it at high sensitive category
     else
     if LOC == MS then
           Place it at medium sensitive category
      else
       if LOC == LS then
           Place it at low sensitive category
        end if
      end if
     end if
     Store locations based on sensitivity
     Generate privacy profile
```

6 Experiments and results

This section provides detail about the implementation and results collection of ESOT. We implement ESOT in Android Studio. We conduct experiments on a smart phone to check different locations on Google map. The method of the proposed ESOT for location obfuscation is described in the following steps.

1. ESOT takes location coordinates on Google map and transform these coordinates to real location.
2. ESOT takes user privacy preferences and based on the user preferences relevant obfuscation level is selected.
3. A range is defined for each level of obfuscation. The system randomly finds another location for obfuscation purpose in this range. The obfuscated location is different from the original location.
4. The obfuscated location coordinates are transferred to real location on Google map. The newly obfuscated location is used to communicate with LBS.

We tested ESOT for three countries, i.e. the United States, the United Kingdom and Pakistan, to show the performance of ESOT and collects the results of real location and obfuscated location in various tables.

Table 2 has the test results for three states in the US: Colorado, South Dakota and New York. Let us explain the obfuscation result for Colorado. In level 1, the distance between the original and obfuscated locations is 271 m, as the search range for location obfuscation begins at 200 m in level 1. We noted the original location coordinates and the obfuscated location coordinates to check variation between the two locations. In level 2, the distance between the original and obfuscated location is 320 m. Similarly, for level 3, the distance is 309 m. The main point of our discussion is that each level of obfuscation searches locations in a certain range; if a location is not found in this range, then the search is extended beyond the range of each level. That is why we found variation in the distance for each level of obfuscation. It is clear from Table 2 that the original location and the obfuscated location are different: hence location privacy is preserved.

Table 3 contains the test results of ESOT for three cities in the United Kingdom: London, Warrington and Edinburgh. Table 3 has the attributes level of obfuscation, original address and its coordinates, obfuscated address and its coordinates, city, and distance between original and obfuscated location. The table contains one level 3 result for Warrington with a distance difference of 500 m. At this level, the distance range is greater than at other levels of different cities. This high difference is because that area is not highly populated or not very detailed on Google Maps.

The experimental results for three cities in Pakistan—Karachi, Lahore and Peshawar—are shown in Table 4. The levels of obfuscation have variation in distance between the original location and the obfuscated location. In the Peshawar district of Pakistan, level 3 obfuscation shows a distance difference of 750 m. This signifies that the area is rural, due to which its obfuscation proximity is increased. It is clear from the table that the original and the obfuscated location are different, which shows efficient privacy protection at each level.

7 Performance comparison

In this section, we provide comparison results of ESOT and SOT [8] for Australia. We provide evaluation results for ESOT in Sect. 7.1, while Sect. 7.2 has evaluation results for SOT [8] for Australia. Section 7.3 contains the comparative Google Map results for SOT [8] and ESOT.

7.1 ESOT evaluation results for Australia

This section describes the results for ESOT for the city of Barcaldine in Australia. The results of three levels of ESOT

Table 2 Experimental results of various states of the United States

Obfuscation levels	Original address	Original location coordinates	Obfuscated address	Obfuscated location coordinates	City/State	Distance (m)
Level 1	2110 William St, Colorado, United States	39.748424489664785 −104.96575970202684	1920 High St, Colorado, United States	39.7461862528253 −104.9645069369716	Colorado	271
Level 2	2224 Franklin St, Colorado, United States	39.750018584020644 −104.96789373457432	1900 Franklin St, Colorado, United State	39.74714288339772 −104.96813107932391	Colorado	320
Level 3	2417 Franklin St, Colorado, United States	39075230268371319 −104.96862899512053	2235 Williams St, Colorado, United States	39.75008399728586 −104.96644770897994	Colorado	309
Level 1	West Hughes SD, South Dakota, United States	44.436061831797524 −100.193983130157	203rd St, South Dakota, United States	44.44030873846342 −100.19751911174595	South Dakota	549
Level 2	West Sully Hughes SD, South Dakota, United States	44.76605643957356 −100.16772530972958	300th Ave, South Dakota, United States	44.761808632344 −100.1621502704478	South Dakota	645
Level 3	29700–29798 177th South Dakota, United States	44.82434516021028 −100.18607128411531	29900–29998 177th South Dakota, United States	44.82549272470636 −100.18195162622544	South Dakota	349
Level 1	80 Gold St, New York, United States	40.7093995420064 −74.00361355394	126–142 John St, New York, United States	40.70733097242514 −74.00533564182037	New York	272
Level 2	10 Reade St, New York, United States	40.714063831908625 −74.00423716753721	93 Worth St, New York, United States	40.716603821691834 −74.0048043372921	New York	287
Level 3	111 Centre St, New York, United States	40.71688048435534 −74.00150567293167	136 Baxter St, New York, United States	40.71869593616287 −73.99874874092922	New York	308

Table 3 Experimental results of various cities of the United Kingdom

Obfuscation levels	Original address	Original location coordinates	Obfuscated address	Obfuscated location coordinates	City/State	Distance (m)
Level 1	Sutton Walk, London, United Kingdom	51.50477768409387 −0.11551637202501297	5 Chicheley St, London, United Kingdom	51.502966238234684 −0.11723325373914692	London	230
Level 2	65 Cut, London, United Kingdom	51.50267359858091 −0.10771483182907104	214 Nelson Square, London, United Kingdom	51.50283245184079 −0.10340491694323707	London	300
Level 3	60 St George’s Rd, London, United Kingdom	51.49595122712448 −0.1033589243888855	52 Lambeth Rd, London, United Kingdom	51.49689044472071 −0.107965678450321	London	340
Level 1	97 Reddish Ln, Warrington, United Kingdom	53.38969000121585 −2.4663525447249413	2 Bollin Dr, Warrington, United Kingdom	53.38746906925341 −2.466494876351478	Warrington	250
Level 2	15 Powder Mill Rd, Warrington, United Kingdom	53.38151912564498 −2.5507868081331253	103 Reynolds St, Warrington, United Kingdom	53.383444071262495 −2.5536348383764027	Warrington	290
Level 3	James St, Warrington, United Kingdom	53.39002551330571 −2.5892607495188713	Lythgoes Ln, Warrington, United Kingdom	53.394550339864985 −2.5897424083032723	Warrington	500
Level 1	1-14 Johnston Terrace, Edinburgh, United Kingdom	55.94861654061588 −3.195297159254551	W Parliament Square, Edinburgh, United Kingdom	55.949056102596224 −3.1914436700524322	Edinburgh	240
Level 2	51 Rose St N Ln, Edinburgh, United Kingdom	55.95231114203605 −3.201479986310005	135 George St, Edinburgh, United Kingdom	55.95208455251182 −3.2058457176097943	Edinburgh	270
Level 3	271 Canongate, Edinburgh, United Kingdom	55.95100255644875 −3.1835122033953667	112−116 Holyrood, Edinburgh, United Kingdom	55.950558568239195 −3.175743770323118	Edinburgh	490

Table 4 Experimental results of various cities of Pakistan

Obfuscation level	Original address	Original location coordinates	Obfuscated address	Obfuscated location coordinate	City/State	Distance (m)
Level 1	Chaba Gali, Karachi, Sindh, Pakistan	24.85567279318369 67.00191579759121	Katchi Gali 2, Karachi, Sindh, Pakistan	24.853913338892102 67.00452438300404	Karachi	330
Level 2	Rehmatullah St, Karachi, Sindh, Pakistan	24.864107290546404 66.99874475598335	Haji Pir Mohammad Rd, Karachi, Sindh, Pakistan	24.864038966010007 66.99620855059831	Karachi	260
Level 3.	Muhammad Ali Alvi Rd, Karachi, Sindh, Pakistan	24.874028633137172 66.99829280376434	Molamabad Ln, Karachi, Sindh, Pakistan	24.8752819802154 66.99546621607305	Karachi	320
Level 1	43 A Luqman St, Lahore, Punjab, Pakistan	31.527878705441232 74.37215443700552	Asad Jan Rd, Lahore, Punjab, Pakistan	31.5245608823333 74.37093534284826	Lahore	390
Level 2	Imtiaz Shaheed Rd, Lahore, Punjab, Pakistan	31.541677082042167 74.37458753585815	Bedian Rd, Lahore, Punjab, Pakistan	31.538280062160247 74.36957020895272	Lahore	610
Level 3	Zarrar Shaheed Rd, Lahore, Punjab, Pakistan	31.549268948553745 74.39523316919804	Street 26, Lahore, Punjab, Pakistan	31.5473746198162 74.39859048962506	Lahore	380
Level 1	Dheri Bagh Banan, Peshawar, KPK, Pakistan	33.9945351418925 33.55522912740707	AjabKhan Afridi Rd, Peshawar, KPK, Pakistan	33.99654728052795 71.5555007682861	Peshawar	230
Level 2	Unnamed Rd, Peshawar, KPK, Pakistan	33.98166617714961 71.58003855496645	District, Peshawar, KPK, Pakistan	33.98201068986116 71.57715305728459	Peshawar	270
Level 3	Sardar Ghari, Peshawar, KPK, Pakistan	34.02077770693353 71.63537487387657	District, Peshawar, KPK, Pakistan	34.02746687473362 71.63477633430055	Peshawar	750

are shown with the help of Table 5. Table 5 contains level of obfuscation, the original address and its coordinates, the obfuscated address and its coordinates, name of city, and distance between original and obfuscated locations. In level 1, the original and the obfuscated addresses have a distance difference of about 230 m. There is variation in the original address coordinates and the obfuscated address coordinates, as clearly shown in the table. At level 2, the distance difference is 350 m, a wider proximity compared with level 1. Similarly, level 3 has a distance difference of 460 m.

7.2 SOT [8] evaluation results for Australia

The results of SOT [8] are described in this section with the help of Table 6. Table 6 contains data for various levels of SOT. Level 1 and level 2 have about same distance difference of 112 m between the original and the obfuscated locations. Level 1 conversion of the original address is based on house number, while at level 2 conversion of the original address is based on street name. At level 3, the distance between the original and obfuscated locations is about 16,556 m. Level 4 has a location distance difference of about 893,260 m. Level 5 has wider proximity at country level, so distance between original and obfuscated is about 3,222,269 m. At level 3, level 4 and level 5, SOT [8] achieves efficient location privacy protection, but greatly degraded location service utility.

7.3 Google Maps results for SOT [8] and ESOT for Australia

This section contains comparative results of SOT [8] and ESOT on Google Maps for Australia at three levels. Figure 4 shows the level 1 results for SOT [8] and ESOT. The original and obfuscated locations are different for both techniques. At level 1, the distance between the original and the obfuscated location is 112 m for SOT [8] and 210 m for ESOT. Similarly, Figs. 5 and 6 show Google Maps results for SOT and ESOT at level 2 and level 3 respectively. These figures clearly show that ESOT has a reasonable distance range which provides efficient privacy protection as well as location services utility.

8 Results analysis

In this section, we compare the results of the proposed ESOT scheme with SOT [8] in terms of privacy protection, balance between privacy and service utility, and generalization.

8.1 Location privacy protection

The comparison results are shown in Table 7. The distance difference percentage between SOT [8] and ESOT in level

Table 5 Experimental results of ESOT for Australia

Obfuscation levels	Original address	Original location coordinates	Obfuscated address	Obfuscated location coordinates	City/State	Distance (m)
Level 1	96 Bauhinia St, Barcaldine, Queensland, Australia	−23.563187789680576 145.28579011559486	66 Beech St, Barcaldine, Queensland, Australia	−23.56154637862665 145.2872038669319	Barcaldine	230
Level 2	68 Elm St, Barcaldine, Queensland, Australia	−23.55436769620168 145.29011484235525	5 Cypress St, Barcaldine, Queensland, Australia	−23.551341817271297 145.28928744195147	Barcaldine	350
Level 3	LOT 2 Fir St, Barcaldine, Queensland, Australia	−23.556025177664 145.28027348220348	219 Oak St, Barcaldine, Queensland, Australia	−23.551974251940255 145.28127364473673	Barcaldine	460

Table 6 Experimental results of SOT for Australia

Obfuscation levels	Original address	Original location coordinates	Obfuscated address	Obfuscated location coordinates	City/State	Distance (m)
Level 1	65–66 Boree St, Barcaldine, Queensland, Australia	−23.56223171143019 145.28828959912062	56–70 Boree St, Barcaldine, Queensland, Australia	−23.563157057604602 145.2878523990512	Queensland	112
Level 2	65–66 Boree St, Barcaldine, Queensland, Australia	−23.56223171143019 145.28828959912062	65–66 Beech St, Barcaldine, Queensland, Australia	−23.563157057604602 145.2878523990512	Queensland	113
Level 3	65–66 Boree St, Barcaldine, Queensland, Australia	−23.56223171143019 145.28828959912062	65–66 Boree St, Patrick, Queensland, Australia	−23.71109582494 83 145.29130574315786	Queensland	16,556
Level 4	65–66 Boree St, Barcaldine, Queensland, Australia	−23.56223171143019 145.28828959912062	65–66 Boree St, Barcaldine, New South Wales, Australia	−31.578474587369563 145.8790659159422	Queensland	893,260
Level 5	65–66 Boree St, Barcaldine, Queensland, Australia	−23.56223171143019 145.28828959912062	38 Willis Street, Wellington, 6011, New Zealand	−41.28714265862147 174.7734526667863	Queensland	3,763,000

1 is 48.70%, which means that ESOT achieves efficient privacy protection at this level. In level 2, the distance difference percentage is 32.29%, meaning that ESOT achieves an improvement in location privacy protection, while in level 3, SOT achieves efficient privacy protection compared with ESOT as it is 3599%, but greatly reduces utility of services. At level 3 of SOT, the user's original location is in one city and the obfuscated location in another, which raises the question of how the user can get the desired location service. Similarly, Table 7 contains results for other cities: Perth and Sydney in Australia. The higher the distance between the original location and the obfuscated location, the higher the location protection will be. To maintain a balance between privacy and service utility, distance should be within a certain range.

Figure 7 shows the comparison of SOT and ESOT in terms of location privacy achievement. The first two levels of ESOT have better performance than SOT in terms of privacy protection. ESOT has higher distance range than SOT, which clearly shows that ESOT has better privacy protection than SOT. However, at level 3, the distance range of SOT reaches 16 km—i.e. the obfuscation location will be another city, which shows that the service utility is greatly degraded. At all three levels, our proposed scheme achieves better performance than SOT in terms of privacy protection and service utility.

We tested our scheme for the city of Perth in Australia, as shown in Fig. 8. The graph clearly shows that at the first two levels ESOT has better distance ranges than SOT, which is a better location privacy achievement, while at level 3, the distance range of SOT reached to 41.6 km, which degrades service utility. So, at all levels, ESOT has a better performance than SOT in terms of location privacy and utility of services.

We also tested both schemes for Sydney in Australia, as shown in Fig. 9. This graph, too, shows that at level 1 and level 2 ESOT has a more suitable distance range than SOT. At level 3, SOT distance range reached to 40.6 km, which is a high achievement in terms of location privacy but utility of service is degraded, while at that level ESOT achieved balance between location privacy and service utility.

8.2 Balance between privacy and service utility

ESOT maintains a balance between privacy and service utility at each level. On the one hand, SOT [8] achieved efficient results for privacy protection at level 3, but greatly reduced service quality. In Table 7, for level 3 in ESOT, the distance difference between the original location and the obfuscated location is 460, 330 and 380 m for Barcaldine, Perth and Sydney respectively, while in SOT this distance is 16,556, 41,622, and 40,933 for Barcaldine, Perth and Sydney respectively, which greatly reduced location service utility. The first

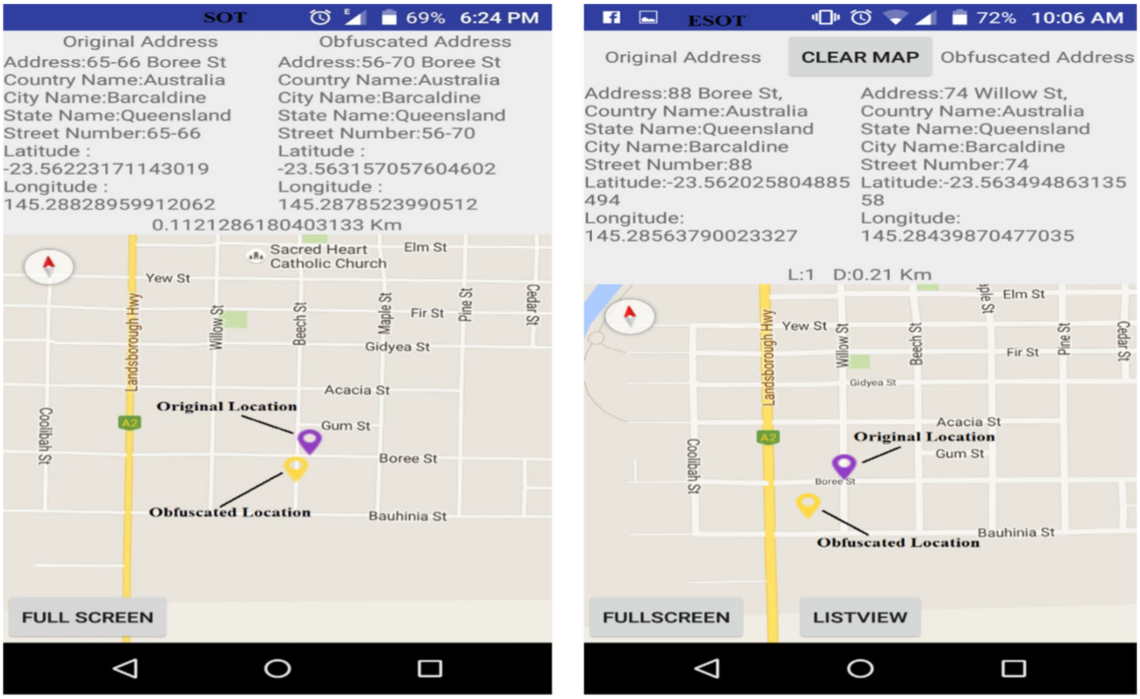

Fig. 4 Level 1 Google Maps results for SOT [8] and ESOT

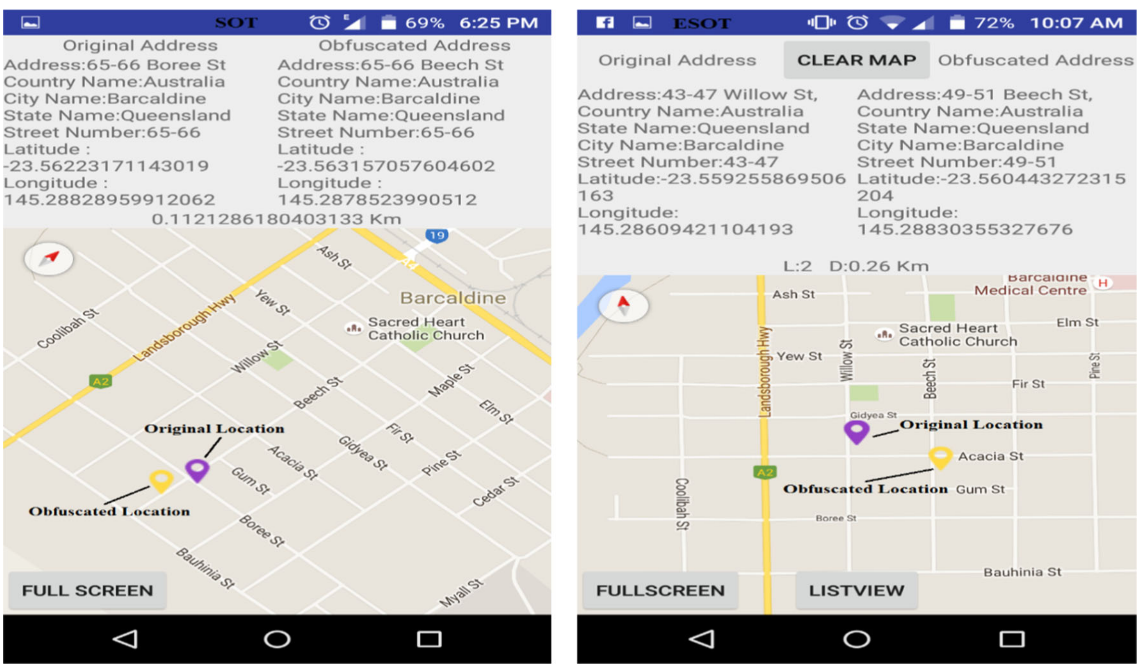

Fig. 5 Level 2 Google Maps results for SOT [8] and ESOT

two levels of SOT improved service utility but reduced location privacy protection, while at level 3 privacy protection is improved but service utility degraded. On the other hand, ESOT achieved improved results to protect location privacy as well as improved service utility. ESOT provides a reasonable distance range between the original and obfuscated locations which maintains balance between privacy and service utility, as clearly shown in Figs. 7, 8 and 9.

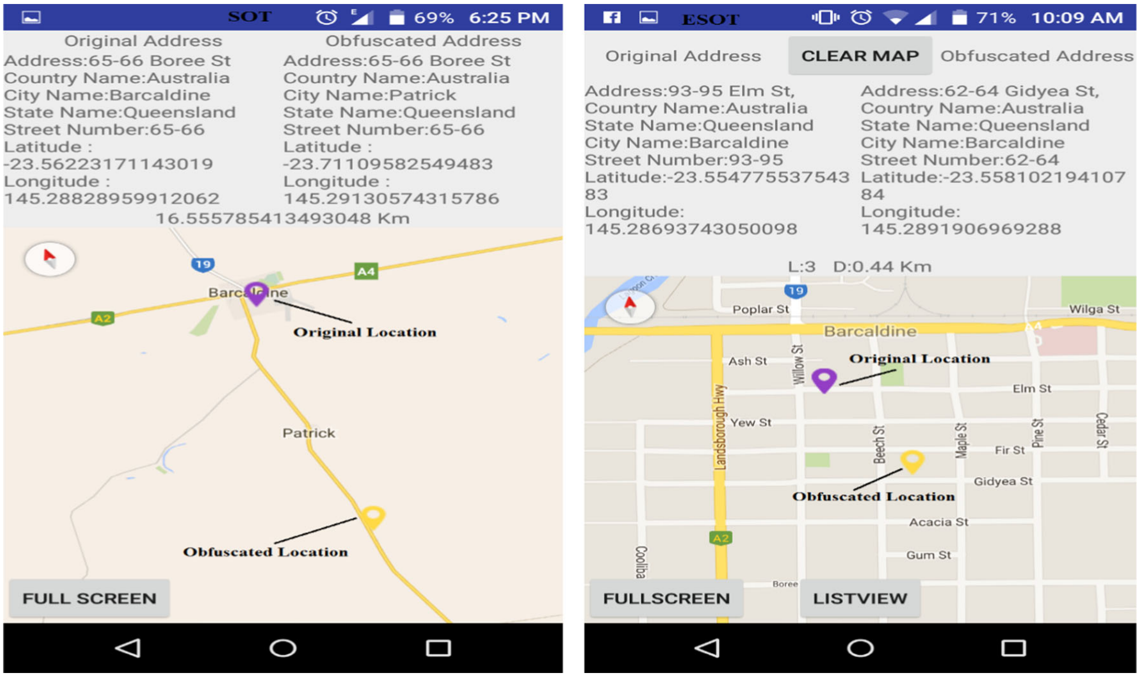

Fig. 6 Level 3 Google Maps results for SOT [8] and ESOT

Table 7 Comparison results of SOT and ESOT

City/State	Level of obfuscation	SOT distance difference in metres	ESOT distance difference in metres	Percentage of distance difference (%)
Barcaldine	Level 1	112	230	48.70
	Level 2	113	350	32.29
	Level 3	16,556	460	3599
Perth	Level 1	106	220	48.18
	Level 2	106	280	37.86
	Level 3	41,622	330	12,612
Sydney	Level 1	186	270	68.88
	Level 2	160	310	51.61
	Level 3	40,933	380	10,771

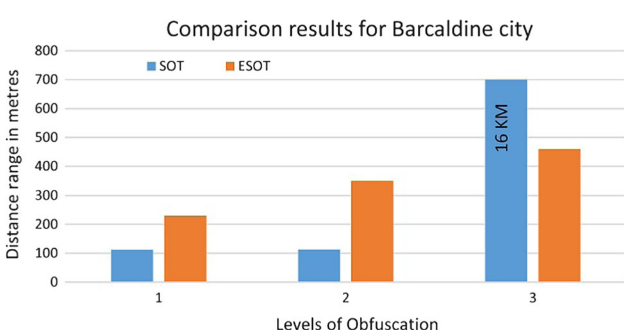

Fig. 7 Comparison of SOT [8] and ESOT for Barcaldine in Australia

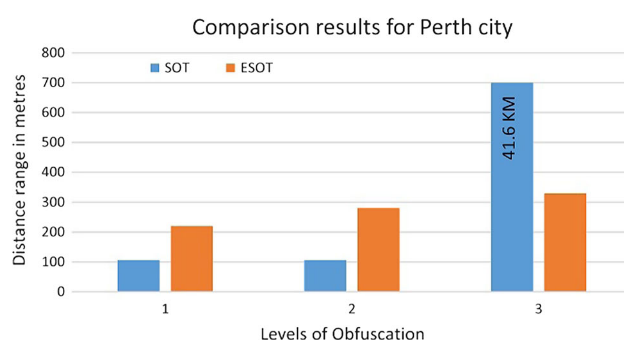

Fig. 8 Comparison of SOT [8] and ESOT for Perth in Australia

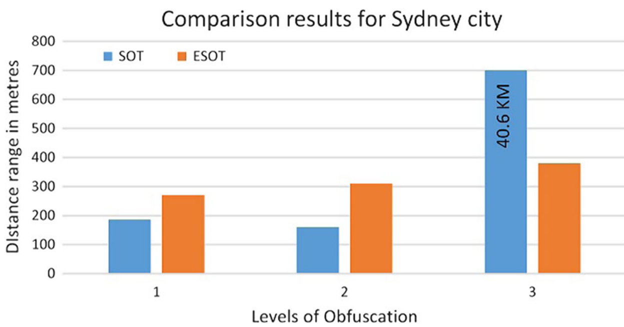

Fig. 9 Comparison of SOT [8] and ESOT for Sydney in Australia

8.3 Generalization

We tested ESOT and SOT for Australia and collected results on Google Maps. SOT [8] is proposed only for Australia. It is difficult to apply SOT [8] all over the world, as the ontology proposed in SOT would be different for different countries and states of the world. Our proposed technique is generalized to be applicable globally on Google Maps. We tested ESOT for four countries, the United States, the United Kingdom, Pakistan and Australia, which shows that ESOT is a generalized technique compared with SOT [8].

Table 8 contains features comparison of four privacy preservation techniques based on various features. Comparing with other techniques, ESOT has improved various features for privacy protection. ESOT efficiently defines levels of sensitivity and user privacy preferences. It also achieves balance between privacy protection and quality of services. ESOT is flexible and could be used globally. As shown in Table 8, other techniques achieve only two or three features regarding privacy protection, while ESOT achieve all the five features in order to protect location privacy in the context of IoT.

9 Conclusion

We proposed a novel technique, ESOT, for location privacy preservation in respect of the Internet of Things. Location privacy is a significant issue to be tackled in light of IoT. We tested our proposed ESOT technique with the help of extensive experiments. Experimental results verify that our ESOT approach attained improved performance compared with SOT in terms of location privacy protection and service utility. The distance range in ESOT between the original location and the obfuscated location is realistic to accomplish balance between location privacy and service utility. ESOT is a general technique and is appropriate globally.

Our new privacy model ESOT achieved the desired result of protecting location privacy. This research work could be extended to take on board the help of longitude (height of

Table 8 Features comparison of various privacy protection techniques

Approach	Privacy levels	Method of protection	Main features	System	Over all achievements				
					Sensitivity levels	Privacy requirements	Flexibility	Balance B/W privacy and quality	Randomization
Proposed ESOT	Three levels	Obfuscation	Sensitivity levels, Privacy protection, service utility, privacy preferences	Internet of Things	✓	✓	✓	✓	✓
θ −RAND [27]	Not mentioned	Obfuscation	Noise based, Randomization	Mobile application		✓			✓
L2P2 [16]	Not mentioned	Anonymization	Diverse privacy requirements	Mobile application		✓	✓		
SOT [8]	Five levels	Obfuscation	Semantic obfuscation	Internet of Things	✓	✓			

buildings) in protecting location privacy. High buildings contain several floors: for this, the original location is converted from one floor in the building to another to hide the actual location of a person or entity. In future, we are also planning to extend levels of obfuscation based on the division of regional areas—i.e. rural area, semi-rural area, urban area and semi-urban area.

Acknowledgements Funding was provided by Directorate for Computer and Information Science and Engineering(Grant No. 61572231).

References

1. Appavoo, P., Chan, M. C., Bhojan, A., & Chang, E.-C. (2016). Efficient and privacy-preserving access to sensor data for Internet of Things (IoT) based services. In *2016 8th International conference on communication systems and networks (COMSNETS)* (pp. 1–8). IEEE.
2. Vermesan, O., & Friess, P. (Eds.). (2014). *Internet of things-from research and innovation to market deployment*. Aalborg: River Publishers.
3. Li, F., Zheng, Z., & Jin, C. (2016). Secure and efficient data transmission in the Internet of Things. *Telecommunication Systems*, *62*(1), 111–122.
4. Park, K. C., & Shin, D.-H. (2017). Security assessment framework for IoT service. *Telecommunication Systems*, *64*(1), 193–209.
5. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks*, *20*(8), 2481–2501.
6. Sun, G., Chang, V., Ramachandran, M., Sun, Z., Li, G., Yu, H., et al. (2017). Efficient location privacy algorithm for Internet of Things (IoT) services and applications. *Journal of Network and Computer Applications*, *89*, 3–13.
7. Sun, G., Huang, S., Bao, W., Yang, Y., & Wang, Z. (2014). A privacy protection policy combined with privacy homomorphism in the internet of things. In *2014 23rd International conference on computer communication and networks* (pp. 1–6).
8. Elkhodr, M., Shahrestani, S., & Cheung, H. (2014). A semantic obfuscation technique for the Internet of Things. In *2014 IEEE international conference on communications workshops* (pp. 448–453).
9. Puttaswamy, K. P. N., Wang, S., Steinbauer, T., Agrawal, D., El Abbadi, A., Kruegel, C., et al. (2014). Preserving location privacy in geosocial applications. *IEEE Transactions on Mobile Computing*, *13*(1), 159–173.
10. Xiao, Q., Chen, J., & Yu, L. (2014). POSTER: LocMask: A location privacy protection framework in android system. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*. ACM.
11. Ullah, I., & Shah, M. A. (2016). A novel model for preserving location privacy in Internet of Things. In *2016 22nd International conference on automation and computing (ICAC)*. IEEE.
12. Sweeny, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(5), 557–570.
13. Gedik, B., & Liu, L. (2008). Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing*, *7*(1), 1–18.
14. Yao, L., Lin, C., Kong, X., Xia, F., & Wu, G. A clustering-based location privacy protection scheme for pervasive computing. In *Proceedings of the 2010 IEEE/ACM international conference on green computing and communications & international conference on cyber, physical and social computing*.
15. Palanisamy, B., & Liu, L. (2011). MobiMix: Protecting location privacy with mix-zones over road networks. In *2011 IEEE 27th international conference on data engineering (ICDE)* (pp. 494–505). IEEE
16. Wang, Y., Li, F., & Xu, B. (2012). L2P2: Location-aware location privacy protection for location-based services. In *INFOCOM, 2012 proceedings IEEE* (pp. 1996–2004).
17. Pan, X., Xu, J., Member, S., & Meng, X. (2012). Protecting location privacy against location-dependent attacks in mobile services. *IEEE Transactions on Knowledge and Data Engineering*, *24*(8), 1506–1519.
18. Vu, K., & Zheng, R. (2012). Efficient algorithms for k-anonymous location privacy in participatory sensing. In *INFOCOM, 2012 proceedings IEEE* (pp. 2399–2407).
19. Che, Y., Yang, Q., & Hong, X. (2012). A dual-active spatial cloaking algorithm for location privacy preserving in mobile peer-to-peer networks. In *2012 IEEE on wireless communications and networking conference (WCNC)*. IEEE.
20. Yang, N., Cao, Y., Liu, Q., & Zheng, J. (2013). CSPC: A context-sensitive personalized collaborative location privacy preserving method. In *Proceedings of the 5th international conference on advanced communication and networking (ACN 2013), Science & Engineering Research Support Society (SERSC)* (Vol. 31, no. Acn, pp. 93–98).
21. Wang, Y., Zhou, H., Wu, Y., & Sun, L. (2012). Preserving location privacy for location-based services with continuous queries on road network. In *2012 7th International conference on computer science & education (ICCSE)*. IEEE No. ICCSE.
22. Niu, B., Li, Q., Zhu, X., Cao, G., & Li, H. (2015). Enhancing privacy through caching in location-based services. In *2015 IEEE conference on computer communications (INFOCOM)* (pp. 1017–1025). IEEE
23. Chen, Y.-M., & Wei, Y.-C. (2012). SafeAnon: A safe location privacy scheme for vehicular networks. *Telecommunication Systems*, *50*(4), 339–354.
24. Nezhad, A. A., Miri, A., Makrakis, D., & Barbosa, L. O. (2009). Privacy within pervasive communications. *Telecommunication Systems*, *40*(3), 101–116.
25. Wightman, P., Coronell, W., & Jabba, D. (2011). Evaluation of location obfuscation techniques for privacy in location based information systems. In *2011 IEEE Latin-American conference on communications (LATINCOM)*. IEEE
26. Dini, G., & Perazzo, P. (2012). Uniform obfuscation for location privacy. In *Data and applications security and privacy XXVI*. Berlin: Springer.
27. Wightman, P., Zurbaran, M., Zurek, E., Salazar, A., Jabba, D., & Jimeno, M. (2013). θ-Rand: Random noise-based location obfuscation based on circle sectors. In *2013 IEEE symposium on industrial electronics and applications (ISIEA)*. IEEE.
28. Wightman, P., Zurbaran, M., & Santander, A. (2013). High variability geographical obfuscation for location privacy. In *2013 47th International Carnahan conference on security technology (ICCST)*. IEEE.
29. Zurbaran, M., Avila, K., Wightman, P., & Fernandez, M. (2015). Near-Rand: Noise-based location obfuscation based on random neighboring points. *Latin America Transactions, IEEE (Revista IEEE America Latina)*, *13*(11), 3661–3667.
30. Xi, Y., Schwiebert, L., & Shi, W. (2006). Preserving source location privacy in monitoring-based wireless sensor networks. In *20th International parallel and distributed processing symposium, 2006. IPDPS 2006*. IEEE.
31. Quercia, D., Leontiadis, I., Mcnamara, L., Mascolo, C., & Crowcroft, J. (2011). SpotME if you can: Randomized responses for location obfuscation on mobile phones. In *2011 31st Interna-*

tional conference on distributed computing systems (ICDCS). IEEE No. Section III.
32. Kachore, V. A., Lakshmi, J., & Nandy, S. K. (2015). Location obfuscation for location data privacy. In *2015 IEEE world congress on services (SERVICES)*. IEEE.
33. Shokri, R., Theodorakopoulos, G., & Troncoso, C. Protecting location privacy: Optimal strategy against localization attacks. In *Proceedings of the 2012 ACM conference on computer and communications security* (pp. 617–627). ACM.
34. Wang, J., Wu, H., & Liu, Y. (2015). A new distributed user-demand-driven location privacy protection scheme for mobile communication network. *International Journal of Distributed Sensor Networks, 2015*, 15. doi:10.1155/2015/743160.
35. Miura, K., & Sato, F. (2013). A hybrid method of user privacy protection for location based services. In *2013 Seventh international conference on complex, intelligent, and software intensive systems (CISIS)* (pp. 434–439). IEEE.
36. Zhu, X., Chi, H., Jiang, S., Lei, X., & Li, H. (2014). Using dynamic pseudo-IDs to protect privacy in location-based services. In *2014 IEEE international conference on communications (ICC)* (pp. 2307–2312). IEEE.
37. Zhou, L., Wen, Q., & Zhang, H. (2012). Preserving sensor location privacy in internet of things. In *2012 Fourth international conference on computational and information sciences (ICCIS)*. IEEE.
38. Khoshgozaran, A., Shahabi, C., & Shirani-mehr, H. (2011). Location privacy: Going beyond K-anonymity, cloaking and anonymizers. *Knowledge and Information Systems*, *26*, 435–465.
39. Agir, B., Papaioannou, T. G., Narendula, R., Aberer, K., & Hubaux, J.-P. (2013). User-side adaptive protection of location privacy in participatory sensing. *Geoinformatica*, *18*(1), 165–191.
40. Oh, S., Vu, T., Gruteser, M., & Banerjee, S. (2012). Phantom: Physical layer cooperation for location privacy protection. In *INFOCOM, 2012 proceedings IEEE* (pp. 3061–3065).
41. Wishart, R., Henricksen, K., & Indulska, J. Context obfuscation for privacy via ontological descriptions. In *Location-and context-awareness* (pp. 276–288). Berlin: Springer.
42. Ardagna, C. A., Cremonini, M., Damiani, E., Vimercati, S. D. C., & Samarati, P. (2007). Obfuscation-based techniques. In *Data and applications security XXI* (pp. 47–60). Berlin: Springer.
43. Ardagna, C. A., Cremonini, M., De Capitani, S., & Samarati, P. (2011). An obfuscation-based approach for protecting location privacy. *IEEE Transactions on Dependable and Secure Computing*, *8*(1), 13–27.
44. Damiani, M. L., Bertino, E., Silvestri, C., & Damiani, M. L. (2008). Protecting location privacy through semantics-aware obfuscation techniques. *Trust Management II*, *263*(I), 231–245.
45. Seidl, D. E., Paulus, G., Jankowski, P., & Regenfelder, M. (2015). Spatial obfuscation methods for privacy protection of household-level data. *Applied Geography*, *63*, 253–263.
46. Ilyas, M., & Vijayakumar, R. (2012). LPM: A distributed architecture and alogorithms for location privacy in lbs. *International Journal of Network Security & Its Applications*, *4*(2), 135.
47. Zhang, Y., Chen, K., & Lian, Y. (2012). A path-based access control method for location obfuscation in mobile environment. In Y. Zhang, & K. Chen (Eds.), *2012 IEEE symposium on electrical & electronics engineering (EEESYM)* (pp. 570–573). IEEE.
48. Skvortsov, P., Frank, D., & Rothermel, K. (2012). Map-aware position sharing for location privacy in non-trusted systems. In *Pervasive computing* (pp. 388–405). Berlin: Springer.
49. Wightman, P. M., Jimeno, M. A., Jabba, D., & Labrador, M. (2012). Matlock: A location obfuscation technique for accuracy-restricted applications. In *2012 IEEE on wireless communications and networking conference (WCNC)* (pp. 1829–1834). IEEE.
50. Le, T., Bao, T., & Dang, T. K. (2012). Semantic B ob-tree: A new obfuscation technique for location privacy protection. In *Proceedings of the 10th international conference on advances in mobile computing & multimedia* (pp. 281–284). ACM.
51. Damiani, M. L., Bertino, E., & Silvestri, C. (2010). The PROBE framework for the personalized cloaking of private locations. *Transactions on Data Privacy*, *3*, 123–148.
52. Haadi, J. A vagueness-based obfuscation technique for protecting location privacy. In *2010 IEEE second international conference on social computing (SocialCom)*. IEEE.
53. Apps, L., Henne, B., Kater, C., Smith, M., & Brenner, M. (2013). Selective cloaking: Need-to-know for. In *2013 Eleventh annual international conference on privacy, security and trust (PST)* (pp. 19–26). IEEE.
54. Elkhodr, M., Shahrestani, S., & Cheung, H. (2013). A contextual-adaptive location disclosure agent for general devices in the internet of things. In *38th Annual IEEE conference local computer networks-workshops* (pp. 848–855).
55. Matt, D., & Kulik, L. (2005). A formal model of obfuscation and negotiation for location privacy. In *International conference on pervasive computing*. Berlin: Springer.
56. David, B., Rarameswaran, E. R., Douglas, M., Andy, A., & Palmer, T. J. (2004). Data obfuscation: Anonymity and desensitization of usable data sets. *IEEE Security & Privacy*, *2*(6), 34–44.
57. Matt, D., & Kulik, L. (2005). Simulation of obfuscation and negotiation for location privacy. In *International conference on spatial information theory* (pp. 31–48). Berlin: Springer.

Ikram Ullah is currently working towards Ph.D. degree with Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan. He received Master of Science in Information Security from COMSATS Islamabad, Pakistan. He received B.Sc. (Computer Science) degree and M.Sc. (Computer Science) degree from University of Peshawar, Peshawar, Pakistan. His research interest includes location privacy in IoT and cross layer design in Underwater Sensor Network.

Munam Ali Shah received B.Sc. and M.Sc. degrees, both in Computer Science from University of Peshawar, Pakistan, in 2001 and 2003 respectively. He completed his MS degree in Security Technologies and Applications from University of Surrey, UK, in 2010, and has passed his Ph.D. from University of Bedfordshire, UK in 2013. Since July 2004, he has been a Lecturer, Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan. His research interests include MAC protocol design, QoS and security issues in wireless communication systems. He received the Best Paper Award of the International Conference on Automation and Computing in 2012. He is the author of more than 50 research articles published in international conferences and journals. He is HEC Approved Supervisor.

Abdul Wahid is Assistant Professor in the Department of Computer Science, CIIT, Islamabad, Pakistan. He has completed Ph.D. from Kyungpook National University, Republic of Korea. He is also reviewer and TPC member of many conferences and journals. He is associate editor of IEEE Access journal. His research interest includes but are not limited to Vehicular Adhoc Network, Wireless Sensor Network, Underwater Wireless Sensor Network, Cyber Physical Systems, Software Defined Networking, Information-centric Networking.

Amjad Mehmood received the Ph.D. degree in Wireless Networks from Kohat University of Science & Technology, Kohat, in 2014. He got virtual postdoc from University of Virginia, USA. Currently, he is perusing his post-doc from Guangdong Provincial Key Laboratory on Petrochemical Equipment Fault Diagnosis, Guangdong University of Petrochemical Technology, Maoming, China. In 2003, he joined the Kohat University of Science & Technology, Kohat, KP, where he's been currently serving as a senior faculty member and the Coordinator of MS/Ph.D. program. He is interested to work in the areas of cyber-physical systems, IoT, connected vehicles, wireless communications and networking, optical communications and networking, smart grid communications and networking, security issues in wireless networks, big data, cloud computing, and fault diagnosis in WSNs. His research wok is supported Guangdong University of Petrochemical Technology, Maoming, China. Dr. Amjad's supervised many students of BCS, MCS, MS and Ph.D. in the above mentioned interests. He's also been remained the part of reviewing and organizing different workshops, seminar, and training sessions on different technologies. Furthermore, he has served as TPC, reviewer, and demo chair for numerous international conferences, including CCNC, SCPA, WICOM, INFOCOM, SCAN, and so on. Additionally, he is a reviewer or associate editor for many peer-reviewed international journals. He has published more than 42 academic articles in peer-reviewed international journals and conferences around the world.

Houbing Song (M'12–SM'14) received the Ph.D. degree in Electrical Engineering from the University of Virginia, Charlottesville, VA, in August 2012. In August 2017, he joined the Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL, where he is currently an Assistant Professor and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us). He served on the faculty of West Virginia University from August 2012 to August 2017. In 2007 he was an Engineering Research Associate with the Texas A&M Transportation Institute. He serves as an Associate Technical Editor for IEEE Communications Magazine. He is the editor of four books, including Smart Cities: Foundations, Principles and Applications, Hoboken, NJ: Wiley, 2017, Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications, Chichester, UK: Wiley-IEEE Press, 2017, Cyber-Physical Systems: Foundations, Principles and Applications, Boston, MA: Academic Press, 2016, and Industrial Internet of Things: Cybermanufacturing Systems, Cham, Switzerland: Springer, 2016. He is the author of more than 100 articles. His research interests include cyber-physical systems, cybersecurity and privacy, internet of things, edge computing, big data analytics, unmanned aircraft systems, connected vehicle, smart and connected health, and wireless communications and networking. He is a senior member of ACM. He was the very first recipient of the Golden Bear Scholar Award, the highest campus-wide recognition for research excellence at West Virginia University Institute of Technology (WVU Tech), in 2016.